A Publicação Mensal de Sensibilizaçao de Segurança para Usuários de Computadores

OUCH!

NESTA EDIÇÃO...

- Você
- Senhas
- Atualização
- Backups

Quatro Passos Para Permanecer Seguro

Visão Geral

Ao mesmo tempo em que a tecnologia ganha um papel importante nas nossas vidas, ela também cresce em complexidade. Dada a rapidez com que as mudanças tecnológicas ocorrem, acompanhar as dicas de segurança pode ser confuso. Parece que há sempre novas orientações sobre o que você deve ou não fazer. No entanto, enquanto os detalhes de como se manter seguro podem mudar ao longo do tempo, há coisas fundamentais que você sempre pode fazer para se proteger. Independentemente da tecnologia que você está usando ou onde você estiver usando, recomendamos os quatro seguintes passos fundamentais. Para saber mais sobre qualquer um dos passos abaixo, consulte a seção “Recursos” no final deste boletim:

Editor Convidado

Ryan Johnson foca em garantir que as organizações estejam preparadas para responder à inevitável violação de segurança. E ensina Análise Forense Avançada de Rede no SANS Institute. Ryan é ativo no Twitter como **@ForensicRJ**.

1. **Você**: Em primeiro lugar, tenha em mente que a tecnologia sozinha não será capaz de te proteger totalmente. Os criminosos descobriram que a maneira mais fácil de burlar até mesmo a tecnologia de segurança mais avançada é lhe atacar. Se eles querem a sua senha, cartão de crédito ou dados pessoais, a coisa mais fácil a fazer é induzir você a dar-lhes essa informação. Por exemplo, eles podem ligar para você fingindo ser do suporte técnico da Microsoft e alegarem que seu computador está infectado, quando na realidade eles são apenas criminosos cibernéticos que querem que você forneça acesso ao seu computador. Ou talvez eles enviem um e-mail explicando que uma encomenda não pôde ser entregue e peçam para clicar em um link para confirmar o seu endereço de correspondência, quando na realidade eles estão induzindo você a visitar um site malicioso que irá invadir seu computador. É assim que os ataques de “sequestro de dados” ou “CEO impostor” começam. Em última análise, a maior defesa contra os atacantes é você. Desconfie sempre. Ao usar o bom senso você pode detectar e parar a maioria dos ataques.

2. **Senhas**: O próximo passo para proteger a si mesmo envolve o uso de uma senha forte e única para cada um dos seus dispositivos e contas online. As palavras-chave aqui são “forte” e “única”. Uma senha forte significa que esta não pode ser facilmente descoberta por hackers ou por seus programas automatizados. Cansado de senhas complexas que são difíceis de lembrar e difíceis de digitar? Tente usar uma frase em seu lugar. Em vez de uma única palavra, use uma série de palavras fáceis de lembrar, como “Onde está meu café?”. Quanto mais longa a sua senha, mais forte ela é. Uma senha única significa usar uma senha diferente para cada dispositivo e conta on-line. Dessa

© SANS Institute 2016

Quatro Passos Para Permanecer Seguro

forma, se uma senha for comprometida, todas as suas outras contas e dispositivos ainda estarão seguros. Não consegue lembrar todas aquelas senhas fortes e únicas? Não se preocupe, nós também não. É por isso que recomendamos que você use um gerenciador de senhas, que é uma aplicação especializada para o seu smartphone ou computador que pode armazenar todas as suas senhas em um formato criptografado.

Ao seguir estes quatro passos-chave, você estará protegendo seus dados por um bom tempo, enquanto aproveita a tecnologia mais recente.

Finalmente, um dos passos mais importantes que você pode tomar para proteger qualquer conta é permitir a verificação em duas etapas. As senhas puramente já não são suficientes para proteger as contas, todos nós precisamos de algo mais forte. Verificação em duas etapas é muito mais forte. Ela usa sua senha, mas também adiciona um segundo passo, relativo a algo que você é (biometria), ou algo que você tem (como um código enviado para seu smartphone ou um aplicativo em seu smartphone que gera o código para você). Ative essa opção em cada conta que você puder, incluindo o seu gerenciador de senhas, se possível. A verificação em duas etapas é provavelmente o passo mais importante que você pode tomar para se proteger e é muito mais fácil do que você pensa.

3. **Atualização**: Certifique-se de que seus computadores, dispositivos móveis, aplicativos e qualquer outra coisa conectada à Internet esteja executando a versão mais recente do software. Os criminosos cibernéticos estão constantemente procurando novas vulnerabilidades no software de seus dispositivos em uso. Quando descobrem vulnerabilidades, eles usam programas especiais para explorá-los e invadir os dispositivos que você está usando. Enquanto isso, as empresas que criaram o software para estes dispositivos estão trabalhando arduamente para corrigi-los, liberando atualizações. Ao assegurar que seus computadores e dispositivos móveis instalam essas atualizações, você torna muito mais difícil para alguém invadi-lo. Para manter-se atualizado, basta ativar a atualização automática sempre que possível. Esta regra aplica-se a quase qualquer tecnologia conectada a uma rede, incluindo TVs, monitores de bebês conectados à Internet, roteadores domésticos, consoles de jogos ou um dia, talvez, até mesmo o seu carro. Se os seus sistemas operacionais ou dispositivos são antigos e não suportam mais atualizações de segurança, recomendamos que você os substitua por novos que suportem essas atualizações.

4. **Backups**: Eventualmente, independente de quão cuidadoso você seja, você pode ter seu equipamento invadido. Se isso acontecer, muitas vezes a única opção para garantir que o seu computador ou dispositivo móvel fique livre

Quatro Passos Para Permanecer Seguro

de malware é limpá-lo totalmente e reconstruí-lo a partir do zero. O atacante pode também impedir que você acesse seus arquivos pessoais, fotos e outras informações armazenadas no sistema invadido. Por isso, muitas vezes a única maneira de restaurar toda a sua informação pessoal é a partir de um backup (cópia de segurança). Certifique-se de que você está fazendo backups regulares de qualquer informação importante e verifique se consegue restaurar os dados a partir deles. A maioria dos sistemas operacionais e dispositivos móveis suporta backups automáticos. Além disso, recomendamos que você armazene seus backups na nuvem ou off-line, para protegê-los contra atacantes cibernéticos.

Saiba Mais

Assine OUCH!, a publicação mensal de sensibilização de segurança, acesse os arquivos de OUCH! e saiba mais sobre as soluções SANS de sensibilização de segurança visitando nossa página em securingthehuman.sans.org/ouch/archives.

Versão Brasileira

Traduzida por: Homero Palheta Michelini, Arquiteto de T/I, especialista em Segurança da Informação - twitter.com/homerop
Michel Girardias, Analista de Segurança da Informação - twitter.com/michelgirardias
Marta Visser – Tradutora autônoma
Rodrigo Gularte, Administrador de Empresas, especialista em Segurança da Informação - twitter.com/rodrigofgularte

Recursos

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Gerenciadores de Senhas:	https://securingthehuman.sans.org/ouch/2015#october2015
Verificação em Duas Etapas:	https://securingthehuman.sans.org/ouch/2015#september2015
Frases Secretas:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

OUCH! é publicado pelo “SANS Securing the Human” e distribuído sob o licenciamento Creative Commons BY-NC-ND 4.0 license. A distribuição ou utilização desta publicação em programas de treinamento é permitida desde que seu conteúdo não seja modificado. Para traduções ou mais informações entre em contato pelo ouch@securingthehuman.org

Board Editorial: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduzida por: Homero Palheta Michelini, Michel Girardias, Rodrigo Gularte, Marta Visser

© SANS Institute 2016